UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,776	02/06/2002	Michael Neuman	2696-001	7550

7590 10/10/2006

Roberts Abokhair & Mardula, LLC
Suite 1000
11800 Sunrise Valley Drive
Reston, VA 20191-5302

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/068,776	**Applicant(s)** NEUMAN ET AL.	
	Examiner Benjamin E. Lanier	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 23 May 2006.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-22,35 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-22 and 35 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s).be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 23 May 2006 amends claims 1, 3, 6, 7, 10, and 18-20. Applicant's amendment has been fully considered and entered.

Response to Arguments

2. Applicant's arguments filed 23 May 2006 have been fully considered but they are not persuasive. Applicant's argument that "He does not have a terminal server between it and the network and therefore He cannot anticipate the claim," is not persuasive because Figure 1 of He shows that the network (element 10) utilizes a security server (element 15) to provide encrypted communications between a user (element 12) and an NE (element 20)(Col. 4, lines 18-30 & Col. 5, lines 27-31).

3. Applicant's argument that He does not disclose encrypting and decrypting critical data transmissions over the network using said intelligent network interfaces is not persuasive because Figure 1 of He shows that the network (element 10) utilizes a security server (element 15) to provide encrypted communications between a user (element 12) and an NE (element 20)(Col. 4, lines 18-30 & Col. 5, lines 27-31).

4. Applicant's argument that "He does not disclose intelligent network interfaces or encryption by said interfaces, this element is not found in He," is not persuasive for reasons set forth above. In addition He shows centrally managing keys and algorithms for encryption/decryption at the security server (Figure 1, element 15 & Col. 4, lines 27-30). Therefore, He discloses **each and every element** of claim 1 and all of the claims dependent thereon.

5. Applicant's argument that "He also lacks any disclosure of a user providing a distinguished name and authentication to a first intelligent network interface attached to the user's host device," is not persuasive because He discloses that the security server verifies the authenticity of a user (Figure 1, element 12 & Col. 4, lines 24-25). The security server receives an identifier and password from a user (element 12) that is checked against information stored in a user profile of the central security database at the security server (Col. 5, lines 8-11).

6. Applicant's arguments with respect to claim 11, mirror previous arguments, and have been fully addressed above.

7. Applicant appears to argue that He's security server cannot read on the claimed intelligent network interface, which is not persuasive because the security server in He is functionally equivalent to the claimed intelligent network interface and therefore meets the claimed limitations.

8. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the present invention works between intelligent network interfaces so it can provide protocol translation, proxy services, etc. without intervention from the CMC. The CMC dynamically distributes servlets) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

9. Applicant's argument that "mere disclosure of an IP network does not disclose protocol translation within a layer or the distribution of servlets to provide the translation," is not persuasive because He discloses that network is an IP (Col. 4, lines 38-40) and therefore utilizes

TCP/IP protocol. TCP/IP protocol contains the application and protocol layers that are also present in ISO 7.

10. Applicant's argument with respect to claim 6 is a repeat of previous arguments, and has been addressed above.

11. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., use of an IPSec Security Parameters Index) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

12. Applicant's argument with respect to claim 8 is a repeat of previous arguments, and has been addressed above.

13. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., allowing an organization to provide hierarchical control over policy creation and dissemination that reflects the hierarchy of responsibility in their organization) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

14. Applicant's argument with respect to claim 10 is a repeat of previous arguments, and has been addressed above.

15. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., functions are

performed by the individual intelligent network interfaces based on policy information dynamically distributed (pushed) from the CMC) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

16. In response to Applicant's argument with respect to claims 12 and 19, the security server of He would also have the claimed features because it is a server coupled to a network (Figure 1).

17. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., an intelligent interface that is capable of enforcing policy on a peer to peer basis independent of a central security sever other than receiving policy requirements) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

18. Applicant's arguments with respect to claim 15 are not persuasive because it has been shown that the security server provides user authentication (above), and that the security server of He utilizes a serial interface.

Claim Rejections - 35 USC § 102

19. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

20. Claims 1-15, 19, 20, 22, 35 are rejected under 35 U.S.C. 102(b) as being anticipated by He, U.S. Patent No. 5,944,824. Referring to claim 1, He discloses a single sign-on system wherein a user obtains access to a plurality of network elements by providing sign-on information (Col. 4, lines 5-18). Each network element has an interface to the network through its own terminal server (Col. 4, lines 31-42), which meets the limitation of providing an intelligent network interface between a network and each device on the network. The security server performs all network security functions for the network (Col. 4, lines 19-20) including data encryption for authentication information and regular traffic data between a user and the network element after a connection is successfully established (Col. 4, lines 27-30 & Col. 5, lines 27-34), which meets the limitation of encrypting and decrypting critical data transmissions over the network using said intelligent network interfaces. The security server acts as a key distribution center (Col. 4, lines 27-30) and contains an encryption algorithm module that stores the encryption algorithm that is used in the encryption procedures (Col. 6, lines 23-28 & Figure 2), which meets the limitation of centrally managing keys and algorithms used by said intelligent network interfaces for encrypting and decrypting critical data transmissions over the network with a central management console.

Referring to claims 2, 4, 5, He discloses that each network element has an interface to the network through its own terminal server (Col. 4, lines 31-42). The secure terminal servers can be considered a gateway or bridging device to connect the network elements to the IP network (Col. 4, lines 41-45), which meets the limitation of each intelligent network interface providing protocol translation based on servlets provided by said CMC, CMC dynamically distributing proxy servlets to intelligent network interfaces based on distinguished name, said servlets selected from the group consisting of SSO servlets, distinguished name firewall servlets, auditing servlets, policy enforcement servlets, and web-filtering servlets.

Referring to claim 3, He discloses that network is an IP (Col. 4, lines 38-40) and therefore utilizes TCP/IP protocol. TCP/IP protocol contains the application and protocol layers that are also present in ISO 7, which meets the limitation of said protocol translation is selected from any two protocols within a single layer of an ISO layer protocol stack.

Referring to claim 6, He discloses that the security server performs all network security functions for the network (Col. 4, lines 19-20) including data encryption for authentication information and regular traffic data between a user and the network element after a connection is successfully established (Col. 4, lines 27-30 & Col. 5, lines 27-34), which meets the limitation of the security servlets are security patching servlets.

Referring to claim 7, He discloses a single sign-on system wherein a user obtains access to a plurality of network elements by providing sign-on information (Col. 4, lines 5-18). Each network element has an interface to the network through its own terminal server (Col. 4, lines 31-42). The security server performs all network security functions for the network (Col. 4, lines 19-20) including data encryption for authentication information and regular traffic data between a user and the network element after a connection is successfully established (Col. 4, lines 27-30 & Col. 5, lines 27-34), which meets the limitation of a first intelligent network interface associated with a first client sending a request to the central management console with the identifying information about a connection that the first client wishes to send to a second client, said information including protocol, distinguished name, service, and header information, said

CMC reviewing said connection against a network policy and determining denial or allowance of said connection. The security server acts as a key distribution center (Col. 4, lines 27-30) and contains an encryption algorithm module that stores the encryption algorithm that is used in the encryption procedures (Col. 6, lines 23-28 & Figure 2), which meets the limitation determining encryption algorithm, authentication required, keys for the connection, if the connection should be redirected to another device, and if the connection needs to be translated, said CMC sending a connection determination, including encryption and authentication algorithms, keys, and any translation servlets required to said first intelligent network interface. The security server establishes mutual authentication between the user and the network element and provides secure communication (Col. 6, lines 1-12), which meets the limitation of said first intelligent network interface initiating said connection with a second intelligent network interface associated with said second client by sending encrypted connection informaiton, said second intelligent network interface querying said CMC with said encrypted connection informaiton received from said first intelligent network interface, including a security parameters index for said connection that uniquely identifies said connection between said first and second intelligent network interfaces.

Referring to claim 8, He discloses a single sign-on system wherein obtains access to a plurality of network elements by providing sign-on information (Col. 4, lines 5-18), which meets the limitation of authentication is a username/password.

Referring to claim 9, He discloses that the security server contains a plurality of security mechanisms (Col. 4, lines 65-67 & Figure 2), which meets the limitation of providing a plurality of CMCs on said network in a hierarchical configuration.

Referring to claims 10, He discloses a single sign-on system wherein a user obtains access to a plurality of network elements by providing sign-on information (Col. 4, lines 5-18), which meets the limitation of a user providing a distinguished name and authentication to a first intelligent network interface attached to the user's host device. Each network element has an interface to the network through its own terminal server (Col. 4, lines 31-42), which meets the limitation of providing an intelligent network interface between a network and each device on the network. The security server performs all network security functions for the network (Col. 4, lines 19-20), which meets the limitation of providing a central management console on said network. The security server verifies the authenticity of the user, and determines the set of network elements that the user is authorized to access (Col. 4, lines 24-28 & Col. 6, lines 57-67), which meets the limitation of the first intelligent network interface verifying the user's authentication with the CMC such that when said user requests services from a second device, the first intelligent network interface requests communication with said second device based on distinguished name, a second intelligent network interface associated with said second device queries the CMC for permission and user authentication for the second device based on distinguished name, the CMC provides user authentication informaiton based on distinguished name to said second intelligent network to allow said second intelligent network interface to log the user into the second device.

Referring to claim 11, He discloses a single sign-on system wherein a user obtains access to a plurality of network elements by providing sign-on information (Col. 4, lines 5-18). Each network element has an interface to the network through its own terminal server (Col. 4, lines 31-42), which meets the limitation of a network, an intelligent network interface between each host device and said network. Several users are connected to the network (Figure 1), which meets the limitation of a plurality of host devices connected to said network. The security server performs all network security functions for the network (Col. 4, lines 19-20) including data encryption for authentication information and regular traffic data between a user and the network element after a connection is successfully established (Col. 4, lines 27-30 & Col. 5, lines 27-34), which meets the limitation of means on each intelligent network interface for encrypting and decrypting critical data transmissions over the network. The security server acts as a key distribution center (Col. 4, lines 27-30) and contains an encryption algorithm module that stores the encryption algorithm that is used in the encryption procedures (Col. 6, lines 23-28 & Figure 2), which meets the limitation of at least one central management console for providing keys and algorithms used by said intelligent network interface for encrypting and decrypting critical data transmissions over the network.

Referring to claims 12, 19, He discloses that the user computer contains a CPU, memory, an I/O interface, and that the network has an I/O interface (Figure 1).

Referring to claims 13, 14, 20, He discloses that each network element has an interface to the network through its own terminal server (Col. 4, lines 31-42), which meets the limitation of each intelligent network interface is implemented in a form of standalone devices.

Referring to claim 15, He discloses that the network interface is a serial port (Col. 4, lines 35-37).

Referring to claim 22, He discloses a single sign-on system wherein a user obtains access to a plurality of network elements by providing sign-on information (Col. 4, lines 5-18), which meets the limitation of a set of dynamically distributed code fragments stored on said CMC for distribution to said intelligent network interfaces, and means on each said intelligent network interface for using said code fragments to provide functions selected of single sign-on.

Referring to claims 35, He discloses a single sign-on system wherein a user obtains access to a plurality of network elements by providing sign-on information (Col. 4, lines 5-18), which meets the limitation of a user providing a distinguished name and authentication to a first intelligent network interface attached to the user's host device. Each network element has an interface to the network through its own terminal server (Col. 4, lines 31-42), which meets the limitation of providing an intelligent network interface between a network and each device on the network. The security server performs all network security functions for the network (Col. 4, lines 19-20), which meets the limitation of providing a central management console on said network. The security server verifies the authenticity of the user, and determines the set of network elements that the user is authorized to access (Col. 4, lines 24-28 & Col. 6, lines 57-67), which meets the limitation of the first intelligent network interface verifying the user's authentication with the CMC, the CMC dynamically distributing a firewall servlets to said intelligent network interface based on said distinguished name.

Claim Rejections - 35 USC § 103

21. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

22. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

23. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over He, U.S. Patent No. 5,944,824, in view of Liu, U.S. Patent No. 6,171,136. Referring to claim 16, He discloses that the network interface is a RS232 serial port (Col. 4, lines 35-37). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a USB serial port interface in He in order to provide a serial port interface that provides for higher data transmission speed than the earlier RS232 serial interface as taught by Liu.

24. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over He, U.S. Patent No. 5,944;824. Referring to claim 17, He discloses that the network interface is a RS232 serial port (Col. 4, lines 35-37), however, it would have been obvious to one of ordinary skill in the art at the time the invention was made in order for the network interface to communicate multiple items of information at one moment, which would reduce operation time.

25. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over He, U.S. Patent No. 5,944,824, in view of Kitazaki, U.S. patent No. 6,172,936. Referring to claim 18, He discloses a single sign-on system wherein a user obtains access to a plurality of network elements by providing sign-on information (Col. 4, lines 5-18) from a user computer (Figure 2). He does not disclose storing the operating system of the user computer on a flash memory.

Kitazaki discloses storing the operating system on a flash memory (Col. 1, line 60). It would have been obvious to one of ordinary skill in the art at the time the invention was made to store the operating system of the user computer on a flash memory in order to obviate the need to transfer the operating system to main memory from the hard disk, which significantly reduces the time required to boot up the computer (Col. 1, lines 61-64).

26. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over He, U.S. Patent No. 5,944,824, in view of Walter, U.S. Patent No. 6,151,677. Referring to claim 21, He discloses that the security server performs all network security functions for the network (Col. 4, lines 19-20) including data encryption for authentication information and regular traffic data between a user and the network element after a connection is successfully established (Col. 4, lines 27-30 & Col. 5, lines 27-34). He does not disclose the encryptor is located on an FPGA. Walter discloses encryption capabilities on an FPGA (Col. 7, lines 29-32). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use an FPGA for encryption purposes in order to provide for inherent tamper protection of the encryption information (Col. 4, lines 55-63).

Conclusion

27. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin E. Lanier